GPIT

Píldora Informativa

TÉCNICA DE ENGAÑO “INGENERIA SOCIAL”

No. 010

Seguridad de la información

Universidad Nacional Abierta y a Distancia

Gerencia de Plataformas e Infraestructura Tecnológica - GPIT

Grupo Funcional Seguridad Informática - GFSI

https://gpit.unad.edu.co/seguridad-de-la-informacion

seguridad.informacion@unad.edu.co

601-3443700 Ext 1687 - 1685

Diciembre 5 de 2023

Introducción

En el vasto panorama de la ciberseguridad, la ingeniería social ha surgido como una amenaza invisible y sutil que se cierne sobre nuestras vidas digitales. A diferencia de los ataques tradicionales que se valen de códigos maliciosos, la ingeniería social se basa en la manipulación psicológica para obtener información confidencial. Este concepto nos sumerge en un mundo donde las artimañas son tan poderosas como la tecnología misma. (Argentina.gob.ar, 2023)

En esta píldora informativa, exploraremos las entrañas de la ingeniería social: qué es, cómo se manifiesta y, lo más importante, cómo podemos defendernos. En un mundo interconectado donde la información es un activo valioso, conocer las tácticas de ingeniería social es crucial para salvaguardar nuestra privacidad y proteger nuestros datos de posibles amenazas.

Acompáñanos en este viaje a través de las estrategias y precauciones que todos debemos tener en cuenta en la era digital para construir una defensa sólida contra aquellos que buscan explotar nuestra confianza. La prevención comienza con el conocimiento, y juntos, podemos fortalecer nuestras defensas contra las artimañas de la ingeniería social.

Objetivo

El propósito principal de esta píldora informativa sobre ingeniería social es empoderar a los lectores con el conocimiento necesario para reconocer, prevenir y contrarrestar las amenazas que surgen a través de tácticas de manipulación psicológica en el ámbito digital. Los objetivos específicos son:

Concientización y Comprensión: Desarrollar una comprensión clara y consciente de qué es la ingeniería social y cómo se manifiesta en diferentes contextos digitales y sociales.

Identificación de Tácticas: Capacitar a los lectores para identificar tácticas comunes utilizadas por ingenieros sociales, como phishing, pretexting y quid pro quo, proporcionando ejemplos prácticos.

Comprender el Impacto: Destacar las posibles consecuencias y riesgos asociados con caer víctima de ingeniería social, desde la pérdida de datos personales hasta el compromiso de la seguridad digital.

Protección Personal y Organizacional: Proporcionar estrategias y buenas prácticas para protegerse contra las tácticas de ingeniería social, tanto a nivel individual como en el ámbito organizacional.

Fomentar la Educación Continua: Incentivar la búsqueda constante de conocimientos en seguridad cibernética y concientizar sobre la importancia de la educación continua para mantenerse a la vanguardia de las amenazas emergentes.

Contribuir a un Entorno Digital Seguro: Motivar a los lectores a aplicar los conocimientos adquiridos en sus interacciones diarias en línea, contribuyendo así a la construcción de un entorno digital más seguro y protegido.

Alcance

La ingeniería social se manifiesta de diversas formas en nuestro entorno digital y cotidiano. En esta píldora informativa, nos enfocaremos en proporcionar una comprensión clara y práctica de los siguientes aspectos:

Definición de Ingeniería Social: Exploraremos en detalle qué implica la ingeniería social y cómo se diferencia de otros métodos de ataque cibernético.

Tácticas Comunes: Analizaremos algunas de las tácticas más utilizadas por los ingenieros sociales, como phishing, pretexting, quid pro quo y su aplicación en redes sociales.

Impacto y Riesgos: Destacaremos las consecuencias potenciales de caer víctima de ingeniería social, desde la pérdida de datos personales hasta el compromiso de la seguridad digital.

Protección y Prevención: Proporcionaremos consejos prácticos y estrategias para protegerse contra las tácticas de ingeniería social, tanto a nivel personal como organizacional.

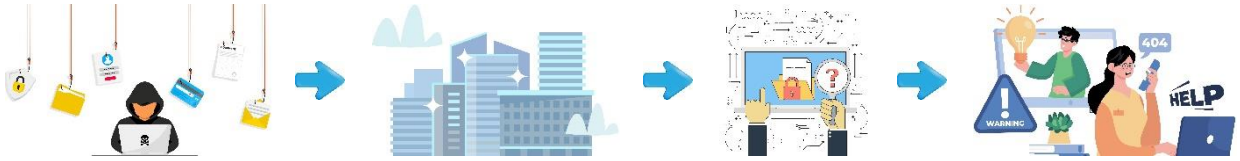
Concientización: Enfatizaremos la importancia de la educación continua y la sensibilización para fortalecer las defensas contra la ingeniería social, tanto en el ámbito laboral como en la vida cotidiana.

Aunque abordaremos estos temas de manera integral, es esencial tener en cuenta que la seguridad digital es un campo en constante evolución. Este recurso proporcionará una base sólida, pero se recomienda mantenerse actualizado mediante recursos adicionales y estar atento a las nuevas tendencias y amenazas que puedan surgir en el futuro.

La meta es equiparte con el conocimiento necesario para reconocer y resistir las tácticas de ingeniería social, contribuyendo así a un entorno digital más seguro y protegido para todos.

Trayectoria de un ataque

En este contexto, nos centramos principalmente en el **punto crítico o método de ataque cibernético** que un ciberdelincuente podría emplear. Este enfoque se dirige hacia la obtención de información, abarcando tanto el ámbito corporativo como el personal. Específicamente, el ciberdelincuente busca acceder a datos confidenciales, ya sea información empresarial estratégica o datos personales de individuos. Esta búsqueda activa de información sensible puede tener diversas finalidades, como el robo de identidad, el espionaje industrial o la realización de actividades fraudulentas. En este escenario, resulta crucial implementar medidas de seguridad cibernética robustas y promover la conciencia sobre las amenazas digitales para salvaguardar la integridad de la información y proteger tanto a entidades corporativas como a individuos.



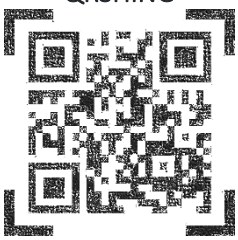
Ciberdelicuente | Objetivo: Entidad | Punto Critico | Engañar

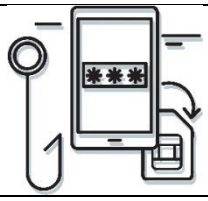
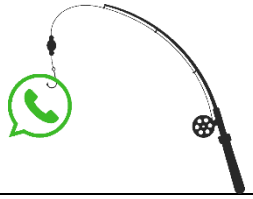
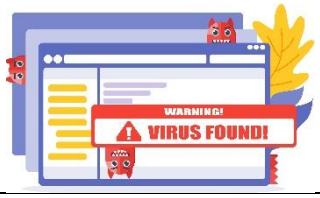
Ciberdelicuente: Es una persona que comete delitos utilizando tecnologías de la información y la comunicación, como computadoras, redes y sistemas electrónicos. Estos individuos aprovechan

vulnerabilidades en sistemas informáticos, redes y programas para llevar a cabo actividades ilegales, como robo de información, fraude, acceso no autorizado a sistemas, difusión de malware, ciberespionaje y otros delitos relacionados con la tecnología.

Objetivo: Entidad: Es mirar sus actividades hacia una entidad especifica, ya sean empresas, organizaciones gubernamentales, instituciones financieras o incluso individuos. Pueden variar según sus motivaciones y metas.

Técnica o punto crítico: Se refiere a la estrategia que un ciberdelincuente emplea de manera continuada a lo largo del tiempo, con el objetivo de engañar a su víctima de manera sistemática. Este enfoque implica la ejecución meticulosa de tácticas específicas durante un extenso período, con el propósito de alcanzar sus metas ilícitas. La persistencia y la cuidadosa planificación son características fundamentales de esta técnica, ya que el perpetrador busca minar la seguridad y confianza de la víctima de manera gradual, con el fin de lograr sus objetivos delictivos. Este método implica una prolongada dedicación por parte del ciberdelincuente, quien busca aprovechar la vulnerabilidad de la víctima mediante un proceso sostenido de manipulación y engaño. (Llorente, 2023)

Técnica o punto critico	Definición
PHISHING 	Es un tipo de ataque cibernético en el que los estafadores engañan a las personas para que revelen información confidencial, como contraseñas, mediante mensajes falsos que parecen legítimos, como correos electrónicos o mensajes de texto. Los atacantes suelen crear sitios web falsos para robar información. La prevención incluye la educación del usuario y la verificación cuidadosa de los mensajes recibidos.
PHARMING 	Es un ataque cibernético en el que los estafadores redirigen el tráfico de usuarios hacia sitios web falsos sin su conocimiento, manipulando el sistema de nombres de dominio (DNS). El objetivo es robar información confidencial al hacer que los usuarios ingresen sus datos en sitios fraudulentos. La prevención implica configurar el DNS de manera segura y utilizar tecnologías anti-pharming.
QRSHING 	A menudo utiliza adhesivos colocados estratégicamente en lugares públicos, como mesas de bares o escaparates de tiendas, con la intención de atraer a personas desprevenidas a escanear los códigos QR. Una vez escaneado, el usuario puede ser redirigido a un sitio web fraudulento que imita la apariencia de una entidad de confianza, con el objetivo de engañar a la víctima para que revele información personal sensible o realice acciones perjudiciales.
SIM SWAPPING	Es una técnica en la que un atacante persuade a la compañía telefónica para que transfiera el número de teléfono de la víctima a una nueva tarjeta SIM bajo su control. Esto puede

	permitir al atacante eludir la autenticación de dos factores y acceder a cuentas vinculadas al número de teléfono.
SMISHING 	Es una combinación de las palabras "SMS" y "phishing". Se refiere a ataques de phishing realizados a través de mensajes de texto, donde los atacantes intentan engañar a las personas para que revelen información confidencial o hagan clic en enlaces maliciosos enviados por SMS.
SPEAR PHISHING 	Es una forma de ataque de phishing altamente personalizada y dirigida. Los atacantes investigan a fondo a la víctima para enviar mensajes engañosos específicamente diseñados para esa persona, aumentando las posibilidades de éxito.
VISHING 	Es una forma de phishing que se realiza a través de llamadas telefónicas. Los atacantes utilizan técnicas de ingeniería social para engañar a las personas y obtener información confidencial.
WHALING 	Se centra en atacar a individuos de alto perfil, como ejecutivos o personas con acceso a información crítica. Estos ataques buscan obtener información sensible o acceso a sistemas importantes.
WHISHING 	Es un término menos común, pero a menudo se utiliza para describir intentos de phishing dirigidos a usuarios de servicios de mensajería como WhatsApp.
HONEYTRAP / CAT PHISHING 	Implica la creación de perfiles falsos en plataformas en línea para atraer a personas y engañarlas. Este tipo de engaño puede involucrar a alguien que se hace pasar por alguien más para manipular emociones y obtener información confidencial.
POP UPS ENGAÑOSOS Y SCAREWARE 	Es una táctica que utilizan ventanas emergentes falsas o mensajes intimidatorios para persuadir a los usuarios de que su sistema está comprometido o infectado, con el objetivo de que descarguen software malicioso.
QUID PRO CUO	Implica ofrecer algo a cambio de información confidencial. Por lo general, el atacante promete algo beneficioso, como soporte técnico o servicios, a cambio de datos sensibles.

	
APLICACIONES MALICIOSAS 	Son programas diseñados para realizar acciones no autorizadas en dispositivos móviles o computadoras. Pueden incluir malware, spyware o adware, y a menudo se distribuyen disfrazadas como aplicaciones legítimas.
USB ABANDONAS 	Conocido como "USB drop attack" o "USB baiting", es una técnica de hacking social que implica dejar dispositivos USB maliciosos en lugares públicos con la esperanza de que alguien los encuentre, los conecte a su computadora y, de esta manera, infecte su sistema o revele información sensible.
WATERING HOLE 	Es una táctica de ataque en la que los ciberdelincuentes infectan los sitios web que saben que su objetivo frecuenta. Al infectar estos "puntos de agua" digitales, esperan atrapar a los visitantes desprevenidos y comprometer sus sistemas.
PIGGBACKING / TAILGATING 	Ocurre cuando un atacante se infiltra en un lugar seguro aprovechando la entrada legítima de otra persona. Puede implicar seguir a alguien a través de una puerta de seguridad sin ser autorizado.

Fuente de las Imágenes: (Shutterstock, s.f.)

Sugerencia

Los funcionarios también desempeñan un papel crucial en la seguridad cibernética. Aquí hay algunas sugerencias y recomendaciones específicas para que contribuyan a la protección de la información:

- ✓ **Concientización y Formación:** Participar activamente en programas de formación y concientización proporcionados. Aprender sobre las amenazas cibernéticas y las mejores prácticas de seguridad es fundamental.
  - Esta actividad se realiza el ultimo jueves de cada mes

- ✓ **Contraseñas Fuertes y Únicas:** Utilizar contraseñas fuertes y únicas para cada cuenta. Evitar el uso de contraseñas comunes y actualizarlas regularmente.
  - https://gpit.unad.edu.co/images/Documentos/109-013_-_Cambio_de_Contrase%C3%B1a_cada_90_d%C3%ADas__Correo_Electr%C3%B3nico_Institucional.pdf

- ✓ **Autenticación Multifactorial:** El uso de la autenticación multifactorial añade una capa adicional de seguridad incluso si la contraseña se ve comprometida.
    - https://gpit.unad.edu.co/images/gpit/109-003_Activacin_MFA.pdf

- ✓ **Evaluación de Correos Electrónicos:** Ser cauteloso al abrir correos electrónicos, especialmente aquellos de remitentes desconocidos o con enlaces y archivos adjuntos sospechosos. No hacer clic en enlaces ni descargar archivos de fuentes no confiables.

- ✓ **Actualizaciones y Parches:** Mantener actualizado el software y los sistemas operativos en dispositivos personales. Las actualizaciones a menudo incluyen correcciones de seguridad importantes.
    - Se sugiere reiniciar el equipo cada ocho días si se mantiene encendido, y durante los fines de semana se aconseja apagarlo

- ✓ **Copia de Seguridad de Datos Personales:** Realizar copias de seguridad regularmente a la información institucional. Esto ayuda a mitigar el riesgo en caso de pérdida de datos debido a un ataque o falla del sistema.
    - Usar la nube privada en Nextcloud

- ✓ **Denunciar Incidentes de Seguridad:** Reportar de inmediato cualquier actividad sospechosa o incidente de seguridad de la informacion
    - Reenviar email a seguridad.informacion@unad.edu.co

- ✓ **Navegación Segura:** Evitar sitios web no seguros y no hacer clic en anuncios sospechosos. Utilizar conexiones seguras (HTTPS) al acceder a sitios web sensibles.

- ✓ **Desarrollar una Mentalidad de Seguridad:** Desarrollar una mentalidad de seguridad al trabajar en línea. Ser consciente de las amenazas y tomar medidas proactivas para proteger la información personal e institucional.

- ✓ **Participar en Pruebas de Concientización:** Participar en simulacros y pruebas de concientización organizados por la institución para evaluar la capacidad de respuesta ante posibles amenazas cibernéticas.

- ✓ **Descargas:** Al realizar descargas, es fundamental aplicar medidas de seguridad, evitando descargar aplicaciones no verificadas.

Referencias

Argentina.gob.ar. (Junio de 2023). *¿Qué es la ingeniería social y cómo me protejo?* Obtenido de https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-la-ingenieria-social-y-

como-protegerte#:~:text=Se%20llama%20ingenier%C3%ADa%20social%20a,haci%C3%A9ndose%20pasar%20por%20otra%20persona.

Llorente, P. G. (16 de Octubre de 2023). *LOS 8 TIPOS DE ATAQUE PHISHING MÁS UTILIZADOS*. Obtenido de https://sellolegal.com/blog/los-8-tipos-de-ataque-phishing-mas-utilizados/

Shutterstock. (s.f.). *Banco de Imagenes*. Obtenido de https://www.shutterstock.com/es/

Elaboro:
Leonardo Montilla Malaver
Líder de Seguridad de la Información

VoBo
Carlos Andrés Materon Serrano
Coordinador GPIT